

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

SHALENE WILLIS, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

LANDMARK ADMIN, LLC, and LIBERTY
BANKERS INSURANCE GROUP,

Defendants.

Case No. 3:24-cv-02741

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Shalene Willis (“Plaintiff”), brings this Class Action Complaint against Defendants Landmark Admin, LLC, and Liberty Bankers Insurance Group (“Defendants”), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to her own actions and her counsel’s investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action complaint against Defendants for its failure to properly secure and safeguard the personally identifiable information (“PII”) and protected health information (“PHI”) (together “Private Information”) of Plaintiff and other similarly situated customers of Defendants (“Class Members”), including their names, addresses, dates of birth, drivers’ license or state-issued ID numbers, passport numbers, Social Security numbers, medical and health insurance information, bank account and routing numbers, and/or life and annuity

policy information. (the “Data Breach”).¹

2. On May 13, 2024, Defendant Landmark discovered malicious activity on its information systems. In response, Landmark purportedly disconnected the systems it believed were affected and began an investigation.²

3. Although Landmark represented that it disconnected affected segments of its information systems, the efforts were apparently not enough because the hackers reportedly regained access to Defendants’ information systems on June 17, 2024.³

4. Though Landmark did not disclose the full scope of its failures in the Notice of Data Breach sent to Plaintiff and the proposed Class Members, Landmark disclosed to authorities that the Breach affected the Private Information of 806,519 people.⁴

5. On information and belief, the attack involved what is commonly referred to as a double-extortion event, which is true of virtually all ransomware attacks in the last few years.⁵

6. Indeed, the “forensic investigation revealed that “data was encrypted and exfiltrated from Landmark’s system.”

7. The cybergang Abyss, who took credit for the attack, is known to commit double-extortion attacks wherein data is first stolen before the hacker group encrypts file in the target’s

¹ Ionut Arghire, *Data Landmark Admin Discloses Data Breach Impacting 800,000 People*, SECURITYWEEK (Oct. 25, 2024), <https://www.securityweek.com/landmark-admin-discloses-data-breach-impacting-800000-people>.

² Exhibit A, Notice of Data Breach Letter to Plaintiff.

³ Ionut, *supra* note 1.

⁴ Office of the Attorney General of Maine, *Data Breach Notifications: Landmark Admin*, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html> (last visited Oct. 30, 2024).

⁵ Cybersecurity and Infrastructure Security Agency, *#StopRansomware*, <https://www.cisa.gov/stopransomware/ransomware-guide> (last visited Oct. 30, 2024) (“Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data. The application of both tactics is known as ‘double extortion.’”).

information systems to take the target offline.⁶

8. After stealing Plaintiff's and Class Members' Private Information, Abyss published a sample list of the Private Information it stole and a note stating that the password would be shared later.



9. Given that Abyss was able to infiltrate Landmark's information systems, perform necessary reconnaissance functions, identify the location of mass amounts of Private Information, exfiltrate all that Private Information, and then perform a comprehensive ransomware encryption event all before Landmark could successfully stop them, it is likely that Landmark lacks the appropriate network intelligence tools to appropriate identify malicious activity on its network or to be able to confirm whether its systems are presently infected—including the appropriate logging, monitoring, and alerting tools such as endpoint detection and response, data loss

⁶ Rebecca Moody, *Landmark Admin Notifies 807k of Data Breach After Ransomware Attack Compromised SSNs, Financial and Medical Info*, COMPARITECH (Oct. 24, 2024), <https://www.comparitech.com/news/landmark-admin-notifies-807k-of-data-breach-after-ransomware-attack-compromised-ssns-financial-and-medical-info>.

preventing, and centralized alerting like a security information and event management tool.

10. Moreover, given that Landmark was aware of the malicious activity in May 2024 but failed to inform affected individuals until October 23—more than five months later—it is likely that Landmark has failed to implement, maintain, and properly test a reasonable cybersecurity incident response plan, which is a foundational element of any reasonable cybersecurity program.

11. Despite Landmark's failure to implement the required cybersecurity safeguards, Liberty Bankers Insurance Group nevertheless chose Landmark as its third-party administrator for insurance carriers. As part of this relationship, Liberty was required by HIPAA to ensure that Landmark had the appropriate cybersecurity measures in place and was required to secure a business associate agreement ensuring the same. Nevertheless, Liberty failed to ensure such measures were in place and failed to reasonably supervise its agent.

PARTIES

12. Plaintiff Willis is a resident and citizen of Newark, New Jersey, where she intends to remain.

13. Defendant Landmark Admin, LLC is a limited liability company organized under the laws of Texas with its principal place of business located at 5750 County Road 225, Brownwood, Texas 76801. The registered agent for service of process is Thomas A. Munson, 5750 County Road 225, Brownwood, Texas 76801. The true identities of Defendants' members are unknown to Plaintiff, who will seek leave to amend to allege such membership. Nevertheless, given the size and scope of Defendants' Data Breach, minimal diversity of the Class Action Fairness Act is present here.

14. Defendant Liberty Bankers Insurance Group is based in Texas with its principal place of business located at 1605 Lyndon B. Johnson Freeway, Suite 700, Dallas, Texas 75234.

JURISDICTION AND VENUE

15. The Court has general subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy is easily more than \$5,000,000 and minimal diversity exists. Specifically, Defendants' failures led to the disclosure of more than 800,000 individuals, so the amount in controversy is met even if merely nominal damages were in controversy. Defendants are citizens of Texas.

16. This Court has personal jurisdiction over Defendants through their business operations in the Dallas Division of the Northern District of Texas, the specific nature of which occurs in this District. Defendants' principal place of businesses are in the Northern District of Texas.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because LBIG's principal place of business is located in the Dallas Division of the Northern District of Texas and a substantial part of the events and omissions giving rise to this action occurred in this District.

ADDITIONAL FACTUAL ALLEGATIONS

18. The information held by Defendants in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

19. Defendants made promises and representations to Plaintiff and Class Members that their Private Information would be kept safe and confidential, and that the privacy of that information would be maintained.

20. Plaintiff's and Class Members' Private Information was provided to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

21. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

Defendants has a legal duty to keep consumer's Private Information safe and confidential.

22. Defendants had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), HIPAA, industry standards, and implicit representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

Defendants' Data Breach Was Imminently Foreseeable

24. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendants, preceding the date of the Data Breach.

25. Data thieves regularly target institutions like Defendants due to the highly sensitive information in their custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

26. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁷

27. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class

⁷ See Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), <https://notified.idtheftcenter.org/s/>.

Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

28. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

29. Defendants was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

30. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

31. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

Healthcare Data Breaches Cause of Substantial Increase in Risk of Medical Fraud

32. The consequences of a company's failure to appropriately protect data is not limited to personally identifiable information. Indeed, healthcare and medical information often causes widespread and devastating consequences for Data Breach victims that they must face for years to come, which causes immediate harm in the form of severe emotional distress at having to face these perils because of someone else's failures.

33. "Consumers should realize that such 'medical identity' fraud can happen in several

ways, from a large-scale breach to individual theft of someone's data.”⁸

34. “If someone gets ahold of another person's health insurance number and driver's license or other ID, they may be able to use it to receive medical services in someone else's name.”⁹

35. “Having your records stolen in a health care data breach can be a prescription for financial disaster. If scam artists break into health care networks and grab your medical information, they can impersonate you to get medical services, use your data to open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.”¹⁰

36. “ID theft victims often have to spend money to fix problems related to having their data stolen, which averages \$600 according to the FTC. But security research firm Ponemon Institute found that health care identity theft victims spend nearly \$13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.”¹¹

37. “Victims of health care data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.”¹²

38. Indeed, Medical Identity Theft is a serious and growing problem in the United

⁸ Michelle Andrews, *Someone Could Steal Your Medical Records and Bill You for Their Care*, NPR (July 26, 2023), <https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself>.

⁹ *Id.*

¹⁰ Brian O'Connor, *Health Care Data Breach: What to Know About Them and What to Do After One*, EXPERIAN (Mar. 31, 2023), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one>.

¹¹ *Id.*

¹² *Id.*

States, causing disruptions in medical care and severe financial issues including medical bankruptcy.¹³

Value of Personally Identifiable Information

39. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁴ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁵

40. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁶

41. For example, Private Information can be sold at a price ranging from \$40 to \$200.¹⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

¹³ U.S. Dep’t of Health and Human Services, *Medical Identity Theft*, <https://oig.hhs.gov/fraud/consumer-alerts/medical-identity-theft>; *The Potential Consequences of Medical Identity Theft Following a Healthcare Data Breach*, DATA BREACH CLASS ACTIONS (July 31, 2024), <https://databreachclassaction.io/blog/the-potential-consequences-of-medical-identity-theft-following-a-healthcare-data-breach>.

¹⁴ 17 C.F.R. § 248.201 (2013).

¹⁵ *Id.*

¹⁶ Anita George, *Your Personal Data Is for Sale on The Dark Web. Here’s How Much It Costs*, DIGITAL TRENDS (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>.

¹⁷ Brian Stack, *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web>.

¹⁸ *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark>.

42. Based on the foregoing, the information compromised in the Data Breach is even more significant because it includes Social Security numbers and other government identification, which is significantly difficult if not impossible to change.

43. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”¹⁹

44. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁰

Defendants Violated its Duties Under HIPAA

45. Defendants is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

46. Defendants is subject to the rules and regulations for safeguarding electronic forms

¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

²⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

of medical information pursuant to the Health Information Technology Act (“HITECH”). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

47. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

48. HIPAA’s Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

49. HIPAA requires “comply[ance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

50. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

51. HIPAA’s Security Rule requires defendants to do the following:

- a. a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. d. Ensure compliance by its workforce.

52. HIPAA also requires Defendants to “review and modify the security measures

implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendants is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

53. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

54. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414, also requires Defendants to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”

55. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Pt. 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

56. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

57. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of

Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302–164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.

58. Defendants was at all times fully aware of its HIPAA obligations to protect the Private Information of consumers yet failed to comply with such obligations. Defendants was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants’ conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Comply with FTC Guidelines

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

60. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

61. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized

access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

64. Defendants was at all times fully aware of its obligation to protect the Private Information of consumers under the FTC Act yet failed to comply with such obligations. Defendants was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Failed to Comply with Industry Standards.

65. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendants as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

66. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendants, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendants failed to follow some or all these industry best practices.

67. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical

security systems; and training staff regarding these points.

68. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

69. Upon information and belief Defendants failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

71. Because of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

72. Indeed, the invasion of Plaintiff's the Class Members' privacy here is particularly

egregious given the scope of medical and health information affected by Defendants' failures.

The Data Breach Increases Victims' Risk of Identity Theft.

73. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendants' failures resulted in Plaintiff's and Class Members' Social Security number falling into the hands of identity thieves.

74. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the Private Information for the express purpose of conducting financial fraud and identity theft operations.

75. Further, the standard operating procedure for cybercriminals is to use some data, like the Social Security numbers here, to access "fullz packages" of that person to gain access to the full suite of additional Private Information that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.²¹

²¹ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm>.

76. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

77. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

78. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendants arguing that the individual failed to mitigate damages.

79. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff’s and Class Members’ Social Security numbers or other government identification are affected.

80. By spending this time, data breach Plaintiff is not manufacturing her own harm,

they are taking necessary steps at Defendants' direction and because the Data Breach included her Social Security number.

81. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

82. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."²²

83. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²³

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

84. Based on the value of the information stolen, the data either has or will be sold to

²² See U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

²³ See Fed. Trade Comm'n, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>.

cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

85. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

86. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their Private Information.

Plaintiff's Experience

87. Plaintiff provided her Private Information to Defendants as a condition of receiving healthcare and insurance services, and Defendants retained Plaintiff's Private Information in its system.

88. Plaintiff was a customer of Liberty Bankers Insurance Group, who then conveyed her information to Landmark.

89. Plaintiff's Private Information was compromised in the Data Breach and stolen by notorious identity thieves who illegally accessed Defendants' network for the specific purpose of targeting the Private Information.

90. Plaintiff takes reasonable measures to protect her Private Information.

91. Because of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She has

and will continue to monitor accounts and credit scores and have sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

92. The Data Breach represents a gross violation of Plaintiff's and the Class Members' Privacy in that Defendants has allowed their most private information to fall into the hands of the exact individuals whose mission it is to misuse that Private Information. The violation of autonomy and control over their own personal details is a blatant and significant violation of privacy, which is a harm on its own that has been recognized in American courts for many decades. Indeed, privacy as a deeply personal expectation is deeply rooted in the U.S. Constitution, including in the Fourth Amendment, and has been long recognized by some of our legal system's greatest minds.²⁴

93. Plaintiff must also now face a substantially increased risk of fraud and identity theft because Defendants has allowed her Private Information, especially her name and Social Security number, being placed in the hands of criminals whose mission it is to monetize that data in the form of identity theft and fraud, even though those thieves often wait a year or more to begin their misconduct.

94. Defendants obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed because of the Data Breach.

95. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Because of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

²⁴ Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

CLASS ALLEGATIONS

96. Pursuant to the Federal Rules of Civil Procedure 23(b)(1), 23(b)(3), Plaintiff brings this action on behalf of herself and on behalf of all members of the proposed class defined as:

All individuals residing in the United States whose Private Information was compromised in the Data Breach and to whom Defendants sent an individual notification that they were affected by the Data Breach (“Class”).

97. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants’ parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

98. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

99. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

100. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes thousands of individuals who have been damaged by Defendants’ conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendants’ records.

101. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

e. Whether Defendants engaged in the conduct alleged herein;

- f. Whether Defendants' conduct violated the FTC Act;
- g. When Defendants learned of the Data Breach;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- i. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- j. Whether Defendants' data security systems, prior to and during the Data Breach, were consistent with industry standards;
- k. Whether Defendants owed duties to Class Members to safeguard their Private Information;
- l. Whether Defendants breached its duties to Class Members to safeguard their Private Information;
- m. Whether hackers obtained Class Members' Private Information via the Data Breach;
- n. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- o. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- p. Whether Defendants knew or should have known its data security systems and monitoring processes were deficient;
- q. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

- r. Whether Defendants' conduct was negligent;
- s. Whether Defendants breached contracts it had with its clients, which were made expressly for the benefit of Plaintiff and Class Members;
- t. Whether Plaintiff and Class Members are entitled to damages;
- u. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- v. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

102. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

103. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

104. Predominance. Defendants has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above

predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

105. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

106. Class certification is also appropriate. Defendants has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

107. Finally, all members of the proposed Class are readily ascertainable. Defendants has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendants' ability to send those individuals notification letters.

CLAIMS FOR RELIEF

COUNT I NEGLIGENCE AND NEGLIGENCE PER SE (On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates the above allegations as if fully set forth herein.

109. Plaintiff and Class Members provided their non-public Private Information to Defendants as a condition of receiving healthcare and insurance services from Defendants.

110. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

111. By assuming the responsibility to collect and store this data, Defendants had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

112. Defendants had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

113. Defendants’ duty to use reasonable security measures also arose under the common law, and as informed by the FTC Act and HIPAA, which mandates that Defendants implement reasonable cybersecurity measures.

114. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

115. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

116. Defendants had and continues to have duties to adequately disclose that the Private Information of Plaintiff and Class Members within Defendants’ possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

117. Defendants breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR, data loss prevention tools, and a centralized security event management system;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- e. Failing to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations; and
- f. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendants to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they

could take appropriate steps to mitigate the potential for identity theft and other damages.

118. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

119. Defendants' violation of the FTC Act and HIPAA also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class Members from the harms associated with data breaches.

120. Defendants has admitted that the Private Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

121. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

122. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

123. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) uncompensated lost time and opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

124. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

125. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

126. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

127. Given Defendants' failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendants' decision not to invest enough resources in its cyber defenses amounts to gross negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates the above allegations as if fully set forth herein.

129. Plaintiff and the proposed Class Members transferred their Private Information to Defendants as part of the agreement to use Defendants' healthcare and insurance services.

130. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information. In exchange, Defendants should have provided adequate data security for Plaintiff and Class Members and implicitly agreed to do so.

131. Indeed, Defendants held itself out as a company dedicated to protecting the privacy of Plaintiff's and the proposed Class Members' Private Information.

132. Defendants knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as a necessary part of receiving financial services.

133. Defendants, however, failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

134. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have allowed it to be provided to Defendants.

135. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory

damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

COUNT III
BREACH OF BAILMENT
(On Behalf of Plaintiff and the Class)

136. Plaintiff incorporates the above allegations as if fully set forth herein.

137. Plaintiff conveyed her Private Information to Defendants lawfully as a condition of receiving financial service with the understanding that Defendants would return or delete her Private Information when it was no longer required.

138. Defendants accepted this Private Information on the implied understanding that Defendants would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiff's Private Information and act on the Private Information only within the confines of the purposes for which Defendants collected Plaintiff's Private Information.

139. By accepting Plaintiff's data and storing it on its systems, Defendants had exclusive control over the privacy of Plaintiff's data in that Plaintiff had no control over whether Defendants' copy of Plaintiff's Private Information was protected with sufficient safeguards and indeed only Defendants had that control.

140. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendants breached this bailment agreement causing harm to Plaintiff in the form of violations of her right to privacy and to self-determination of who had/has access to her Private Information, in the form of requiring her to spend her own valuable time responding to Defendants' failures,

and in the form of forcing Plaintiff and the Class to face years of substantially increased risk of identity theft and financial fraud.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

141. Plaintiff incorporates the above allegations as if fully set forth herein.

142. Plaintiff and Class members took reasonable and appropriate steps to keep their Private Information confidential from the public.

143. Plaintiff and Class members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

144. Defendant owed a duty to its consumers, including Plaintiff and the proposed Class Members, to keep their Private Information confidential.

145. The unauthorized release of Private Information, especially protected health information, is highly offensive to any reasonable person.

146. Plaintiff's and Class members' Private Information is not of legitimate concern to the public.

147. Defendant knew or should have known that Plaintiff's and Class members' Private Information was private.

148. Defendant publicized Plaintiff's and Class members' Private Information, by communicating it to cybercriminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web and other malicious channels of communication (e.g., Telegram and Signal).

149. It is therefore substantially certain that the Plaintiff's and the Class members' Private Information is rapidly becoming public knowledge—among the community writ large—due to the nature of the malware attack that procured it, and the identity theft that it is designed for.

150. Moreover, because of the ubiquitous nature of data breaches, especially in the healthcare industry, Defendant was substantially certain that a failure to protect Private Information would lead to its disclosure to unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship to Plaintiff and the proposed Class Members—in that those identity thieves are precisely the individuals whose aim it is to misuse such Private Information.

151. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiff and Class members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiff's and Class members' privacy by Defendant.

COUNT V
THIRD-PARTY BENEFICIARY
(On Behalf of Plaintiff and the Class)

152. Plaintiff incorporates the above allegations as if fully set forth herein.

153. In procuring the services of Defendant Landmark, Defendant Liberty was required to enter into a business associate agreement with Landmark to require that Landmark implement reasonable cybersecurity requirements detailed in HIPAA's implementing regulations.

154. Such contract was entered into for the benefit of Plaintiff and the Class Members and to protect their health privacy.

155. Landmark's failure to implement reasonable cybersecurity safeguards, as detailed above, is a breach of that contract, which was entered into for Plaintiff's and the Class Members' benefit.

156. The breach of that contract has caused and will continue to cause widespread harm to Plaintiff and the Class, including a gross privacy violation and an increased risk of identity theft and fraud which Plaintiff and the Class must be reimbursed their expenses and otherwise compensated for the efforts they must expend to protect themselves because of Defendants' failures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendants and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

- ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
 - v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
157. requiring Defendants to audit, test, and train its security personnel regarding any

new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

- i. requiring Defendants to conduct regular database scanning and securing checks;
- ii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- iii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- iv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- v. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- vi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
- vii. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;
- E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
- F. Pre- and post-judgment interest on any amounts awarded; and
- G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a trial by jury on all issues so triable.

Dated: October 31, 2024

Respectfully submitted,

/s/ Joe Kendall

Joe Kendall (TX Bar No. 11260700)
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, TX 75219
Tel: 214-744-3000
jkendall@kendalllawgroup.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

Counsel for Plaintiff and the Proposed Class
**pro hac vice forthcoming*